Independent Security Operations, Oversight and Assessment (ISOO&A) Support

Performance Work Statement (PWS)

(DRAFT)

Table of Contents

Independent Security Operations, Oversight and Assessment (ISOO&A) Support

Performance Work Statement (PWS)

1.0 Scope

The Department of the Navy (DON) operates the largest intranet in the world which connects to the Global Information Grid (GIG) along with many other information systems. Naval networks provide end to end secure Information Technology (IT) Services to more than 700,000 users across 3,000 locations worldwide from major bases to single-user locations. In 2010, the enterprise will support, at a minimum, the following:

- Approximately 400,000 seats (desktop and laptops)
- Six (6) locations as defined in Enclosure (1)
- Approximately 50 classified and unclassified Server Farms providing over 1,070 Terabyte (TB) storage capacity
- Over 3,000 enterprise wide servers
- Over 20,000 Blackberry wireless devices and 5,000 Air Cards

The DON network can support both Unclassified and Classified network environments as separate entities. All classified and unclassified locations as outlined in enclosure (1). Communications beyond DON networks will be provided through secure interfaces to the Secret Internet Protocol Routing Network (SIPRNET) or to the Non-Secure Internet Protocol Router Network (NIPRNET) to excepted and legacy networks.

With the services outlined in this PWS, the DON will obtain increased visibility into network operations by conducting comprehensive security assessments and independent Verification, Validation and Reporting (VV&R) at the network operational nodes and other select sites throughout the enterprise. The scope of the ISOO&A Services will provide the DON with a continuous, comprehensive assessment program with the ability to support all DON networks.

2.0 General Requirements

The contractor shall provide scheduling, planning, penetration testing/auditing and reporting services on DON networks. These services are outlined in this PWS and are grouped into the following four separate phases:

- Scheduling
- Planning
- Penetration Testing/Auditing
- Reporting

2.1 Scheduling

The contractor shall submit an initial resource loaded schedule within 60 days of contract award and a Work Breakdown Structure (WBS), to at least the fourth level, with a Data Dictionary which will be the basis of the proposed schedule. At time of solicitation for the base year and no later than 1 June prior to the start of each Option Year, the government will provide the contractor with: (1) which sites from enclosure 1 of this PWS are to be visited that year; and (2) which test/audits from 3.2 of this PWS are to be conducted at each site. Based on that direction, the contractor shall develop a schedule, using Microsoft Office Project 2007 (and/or current government-approved tool), to include the audit/test start and projected end dates and number of individuals traveling for each of the sites to be visited during each government Fiscal Year (FY). Option Year schedules shall be submitted no later than 15 July prior to each option year. The contractor shall make any government directed changes to the schedule and obtain approval of the final schedule from the Contracting Officer Representative (COR) no later than 15 September of each year. After final approval of the FY schedule, the contractor shall provide any recommended changes and obtain approval of any changes from the COR in writing. The schedule shall include no more than four trips to locations outside of the continental United States unless additional (OCONUS) locations are directed by the Government to be included in the schedule.

2.2 Planning

2.2.1 Planning for Penetration Test/Audit

Fifteen (15) days prior to conducting a Penetration Test/Audit, the contractor shall develop and submit to the government for approval a penetration test/audit plan for the designated site visit including the rules of engagement for that test/audit. The rules of engagement shall not impact the normal operation of the site to end-users. The test/audit plan shall include recommended data items that will be included in any interim or final reports submitted as a result of the test/audit and a proposed reporting format. The Contracting Officer or the Contracting Officer Representative shall be the only person(s) with the authority to approve test/audit plans and deviations/modifications to test/audit plans. All test/audit plans (and modifications/deviations) shall be approved in writing. The contractor may be required to conduct site visits during the process of developing a test/audit plan. The DON Assistant Program Manager (APM) Cyber Security Information Assurance (CSIA) will provide the contractor access to ISOO&A project information (passwords, user ID's, etc.).

The contractor shall develop procedures and methods to be used in each test/audit and include these procedures in each plan as well as what equipment will be used. Proposed procedures shall be in accordance with accepted industry practices. The contractor shall obtain a list of approved devices and software from the government and include the list in each plan.

2.3 Penetration Testing/Auditing

After the contractor has obtained an approved penetration test/audit plan from the government for a designated site, the contractor shall conduct the test/audit in accordance with the approved plan. Tests and audits may include large locations such as military locations, functional locations such as Network Operating Centers, Server Farms, or other aspects of the network as directed by the government. Tests and audits will be accomplished in accordance with Section 3 of this PWS and may include penetration tests/audits on multiple service providers which could involve the government, DON contractor or other third party as identified participants in the plan. Penetration testing inclusive of rules of engagement for red, green and blue team exercises and auditing may be required at a government or contractor site as delineated in the plan.

2.4 Reporting

2.4.1 Penetration Test/Audit Reporting

The contractor shall provide a penetration test/audit report to the government. The report will be in the format that was approved in the audit/test plan and includes, at a minimum, all information identified in the government approved plan. The report will be submitted in accordance with the guidelines identified in 2.4.1.1. In the event that a CAT-1 finding is identified, an exception report will be submitted to the government in accordance with the guidelines identified in 2.4.1.2. Any changes to the reporting requirements, whether recommended by the contractor or directed by the government, shall be approved in writing by a modification to the plan. Reports shall be classified as either a standard report or an exception report as follows:

2.4.1.1 Standard Report

The contractor shall submit all standard reports within ten business days of the scheduled completion date of the penetration test/audit. In the event the actual completion date is later than the scheduled completion date, upon approval from the government, the standard report shall be submitted within ten (10) days of the actual completion date. The standard report shall be in accordance with the requirements of the approved test plan and CDRL IAS001. In the event of a discrepancy, the government approved plan will take precedence.

2.4.1.2 Exception Report

The contractor shall submit an exception report within 24 hours of a CAT-1 class finding. A CAT-1 class finding is defined as a security control vulnerability which may allow primary security protections to be bypassed, allowing immediate access by unauthorized personnel or unauthorized assumption of super-user privileges. The exception report shall be in accordance with the requirements of the approved test

plan and CDRL IAS002. In the event of a discrepancy, the government approved plan will take precedence.

2.4.2 Monthly and Annual Summary Reporting

The contractor shall provide a monthly summary report and an annual summary report to the government. The report will be submitted in accordance with the guidelines identified in 2.4.2.1 and/or 2.4.2.2, as applicable. Any changes to the reporting requirements, whether recommended by the contractor or directed by the government, shall be approved in writing by the Contracting Officer.

2.4.2.1 Monthly Summary Reporting

The contractor shall submit a monthly summary report on or before the 5th day of each calendar month following contract award. The monthly reports will be delivered in an electronic format and include the latest version of the updated Microsoft Office Project 2007 schedule, reporting standard scheduling fields and information, as established by the program. The latest version of the updated Microsoft Office Project 2007 schedule will be available on the program's data portal for read-only access by all program team members. The monthly summary report will contain, at a minimum, all information identified in CDRL IAS003.

2.4.2.2 Annual Project Summary Reporting

The contractor shall submit an annual project summary report within the last (30) days of each annual contract period. The annual summary report will contain, at a minimum, all information identified in CDRL IAS004.

3.0 Detailed Requirements

Each penetration test/audit conducted by the contractor shall be in accordance with this PWS. The following areas have been identified as the core areas that shall be tested/audited. The penetration test for the Red, Blue, and Green Exercises detailed in 3.1 below is the only test to be performed by the contractor in this PWS. The remaining tasks detailed in 3.2 through 3.27 are audits to be performed by the contractor and represent the bulk of the effort required under this contract. Each plan submitted by the contractor in 2.2 shall identify which of the areas shall be included in the specific penetration test/audit. The penetration test will include the specific tasking in 3.1. The audits, depending on their location or purpose, will include some or all of the specific tasking in 3.2 through 3.27. When directed by the government and approved in the plan, the contractor shall conduct both the penetration test in 3.1 and an audit to include some or all of the specific tasking in 3.2 through 3.27.

3.1 Penetration Tests/Red, Blue and Green Team Exercises

The contractor shall:

a. perform Red, Blue, and Green Team exercises as defined in Enclosure (2) of this PWS in accordance with the NIST SP800-115, "Technical Guide to Information Security Testing and Assessment" or the equivalent follow-on or replacement technical guidance.

3.2 Inventory of Authorized and Unauthorized Devices

The contractor shall conduct auditing, in accordance with the approved test plan, to verify that:

a. devices connected to the network are in accordance with the government provided list of approved devices.
b. devices connected to the network maintain the "state of the shelf," as defined in the Enclosure (2) of this PWS.

3.3 Inventory of Authorized and Unauthorized Software

The contractor shall conduct auditing, in accordance with the approved test plan, to verify that:

a. software used on the network is in accordance with the government provided list of approved software.
b. the most current version of the operating system security patches, application patches, and hardware basic input/output system **(**BIOS**)** updates are installed. The contractor shall use only a DoD/DON approved tool to conduct this test.
c. the signature files for associated host-based Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are no more than two (2) days old.
d. implemented white lists and black lists as defined in Enclosure (2) of this PWS are no more than thirty (30) days old.

3.4 Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers

The contractor shall conduct auditing, in accordance with the approved test plan, to verify that:

a. any computer system re-imaged for use on the site's network uses the most current approved, standardized image as designated by the government.

3.5 Secure Configurations for Network Devices

The contractor shall conduct auditing, in accordance with the approved test plan, to verify that:

a. any deviations from the documented baseline have been approved by the DON Change/Configuration Control Board (CCB).

b. the DON CCB membership includes the system Information Assurance Manager (IAM).
c. all internal Domain Naming System (DNS) servers are configured to resolve unresolved requests to the DNS located in a protected Demilitarized Zone (DMZ).

3.6 Boundary Defense

The contractor shall conduct auditing, in accordance with the approved test plan, to verify that:

a. the designated site's implementation of Defense-in-Depth strategies at the B1 boundary complies with Chapter 3 of the "DON CIO Information Technology Standards Guidance (ITSG)" and Appendix E of the "DON CIO Information Technology Infrastructure Architecture (ITIA)" or the equivalent follow-on or replacement technical guidance, as provided by the government.

3.7 Maintenance, Monitoring, and Analysis of Audit Logs

The contractor shall conduct auditing, in accordance with the approved test plan, to verify that:

a. audit logs are aggregated to a centralized logging server in accordance with GAO-09-232G, "Federal Information System Controls Audit Manual" or the equivalent follow-on or replacement technical guidance.
b. the site IAM reviews the audit logs for exceptions in accordance with DoDI 8500.2, "IA Control Checklist – MAC 1- Classified" or the equivalent follow-on or replacement technical guidance.

3.8 Controlled Use of Administrative Privileges

The contractor shall conduct auditing, in accordance with the approved test plan, to verify that:

a. the accounts with elevated privileges are used exclusively for administrative purposes.
b. the designated site implements and complies with the password complexity rule set in accordance with DoDI 8500.2, "IA Control Checklist – MAC 1-Classified" or the equivalent follow-on or replacement technical guidance.

3.9 Controlled Access Based on Need to Know

The contractor shall conduct auditing, in accordance with the approved test plan, to verify that:

a. user access is implemented based upon the "Need to Know" methodology as defined in Enclosure (2) of this PWS.

3.10 Continuous Vulnerability Assessment and Remediation

The contractor shall conduct auditing, in accordance with the approved test plan, to verify that:

a. the designated site is implementing the DON Information Assurance Vulnerability Management (IAVM) Program in accordance with DoDI 8500.2, "IA Control Checklist – MAC 1- Classified" or the equivalent follow-on or replacement technical guidance.
b. any IAVM program actions not implemented are documented in a Plan of Action & Milestones (POA&M).
c. the last five Communications Tasking Orders (CTOs), Government Directed Actions (GDA), and Operational Directives (OpDir), as provided by the government, are implemented.
d. administrative/domain credentials for scanning networks are being implemented.
e. the designated site complies with DON Computer Network Incident Response and Reporting Requirements in accordance with SECNAVINST 5239.19 or the equivalent follow-on or replacement technical guidance.

3.11 Account Monitoring and Control

The contractor shall conduct auditing, in accordance with the approved test plan, to verify that:

a. the designated site has a documented access control management policy and it is implemented in accordance with NIST SP 800-53 revision 3 or the equivalent follow-on or replacement technical guidance.
b. the designated site's active directory identifies all users with a last log-on date greater than or equal to 90 days.
c. the designated site's Certificate Revocation List (CRL) is no older than one month.

3.12 Malware Defenses

The contractor shall conduct auditing, in accordance with the approved test plan, to verify that:

a. the designated site's signature files for both anti-virus and anti-malware are no older than two days.
b. the designated site's incident reporting timelines are in accordance with SECNAVINST 5239.19 or the equivalent follow-on or replacement technical guidance.

3.13 Limitation and Control of Network Ports, Protocols, and Services

The contractor shall conduct auditing, in accordance with the approved test plan, to verify that:

a. the designated site complies with DoDI 8551.1, “Ports, Protocols, and Service Management (PPSM)” and/or “Navy Unclassified Trusted Network Protection (UTNProtect) Policy” or the equivalent follow-on or replacement technical guidance, as provided by the government.

3.14 Wireless Device Control

The contractor shall conduct auditing, in accordance with the approved test plan, to verify that:

a. the designated site’s wireless devices comply with DoD wireless policy contained in DoDD 8100.2, “Guidance on the Implementation of Wireless Technologies within the Global Information Grid (GIG)” or the equivalent follow-on or replacement technical guidance.

3.15 Secure Network Engineering

The contractor shall conduct auditing, in accordance with the approved test plan, to verify that:

a. the network diagrams, as provided by the government, reflect the designated site’s current network topology.
b. the designated site’s network diagrams include the following information:
    1. Building and locations.
    2. Server names.
    3. Complete IP addresses.
    4. Cross Domain Solutions.
    5. Circuit Identifiers.
    6. Routers.
    7. Switches.
    8. IA equipment providing protection.
    9. Any external interfaces except the command communications service designator (CCSD).
c. the designated site’s access to websites on the Internet are routed through a perimeter that includes firewall, IDS, web proxy, packet inspection, packet logging functionality, and session reconstruction capabilities.
d. the designated site complies with the regulations for Public Key Infrastructure (PKI) services processes, procedures, and documentation in accordance DoD Instruction 8520.2 or the equivalent follow-on or replacement technical guidance.

3.16 Incident Response Capability

The contractor shall conduct auditing, in accordance with the approved test plan, to verify that:

a. the designated site's plans, policies, procedures, and documentation for incident response comply with SECNAVINST 5239.19 or the equivalent follow-on or replacement technical guidance.
b. the designated site employs automated mechanisms to detect and report incidents in compliance with Chapter 3 of the "DON CIO Information Technology Standards Guidance (ITSG)" and Appendix E of the "DON CIO Information Technology Infrastructure Architecture (ITIA)" or the equivalent follow-on or replacement technical guidance, as provided by the government.
c. incidents are monitored and escalated in accordance with the designated site's escalation procedures and policies, as provided by the government.
d. the designated site's plans, policies, procedures, and documentation concerning classified/non classified spillage cleanup comply with CNSS Policy No.18, June 2006 or the equivalent follow-on or replacement technical guidance.

3.17 Data Restoration Capability

The contractor shall conduct auditing, in accordance with the approved test plan, to verify that:

a. the designated site's backup tapes are stored offsite in a way that prevents loss from natural disaster in compliance with SECNAV M-5239-1 section 4 or the equivalent follow-on or replacement technical guidance.

3.18 Security Skills Assessment and Appropriate Training

The contractor shall conduct auditing, in accordance with the approved test plan, to verify that:

a. the security skills and staff training at the designated site comply with the baseline knowledge and skills required by DoD 8570.01M or the equivalent follow-on or replacement technical guidance.

3.19 Command and Control (C2) Tools and Processes

The contractor shall conduct any testing and/or auditing required to verify that:

a. the designated site's C2 planning, executing, and reporting tools are in use and comply with a documented set of operating procedures in accordance with the Naval Network Warfare Command C2 policy, as provided by the government.

3.20 Personally Identifiable Information (PII)

The contractor shall conduct auditing, in accordance with the approved test plan, to verify that:

a. no Personally Identifiable Information (PII) records at the designated site are routinely processed or stored on mobile computing devices or removable electronic

media without the written consent of the DAA in accordance with "DoD PII Guide," 18Aug2006 or the equivalent follow-on or replacement technical guidance.
b. all sensitive PII records at the designated site are encrypted to provide record protection accordance with the "DoD PII Guide," 18Aug2006 or the equivalent follow-on or replacement technical guidance.
c. any loss (or suspected loss) of PII at the designated site is reported in accordance with paragraphs 4.3 and 4.4 of the "DoD PII Guide," 18Aug2006 or the equivalent follow-on or replacement technical guidance.
d. the designated site conducts Privacy Impact Assessments (PIAs) in accordance with section 208 of the e-government Act of 2002 or the equivalent follow-on or replacement technical guidance, as provided by the government.

3.21 Privacy and Security Safeguards/Security Architecture

The contractor shall conduct auditing, in accordance with the approved test plan, to verify that:

a. all documents, equipment, and machine-readable media containing classified data maintained at the designated site are cleared and sanitized before release outside its security domain using procedures in accordance with DoD 5200.1-R and DoDI 8500.2 or the equivalent follow-on or replacement technical guidance.
b. all documents, machine-readable media, and equipment maintained at the designated site are destroyed using procedures in accordance with DoDI 5200.1-R and DoDI 8500.2 or the equivalent follow-on or replacement technical guidance.

3.22 Media Protection

The contractor shall conduct auditing, in accordance with the approved test plan, to verify that:

a. the proper marking and storage of removable media devices when not in use at the designated site are in accordance with DoDI 8500.2 or the equivalent follow-on or replacement technical guidance.
b. only government-owned and controlled media at the designated site are used on agency information systems regardless of classification in accordance with DoDI 8500.2 or the equivalent follow-on or replacement technical guidance.
c. review storage process at the designated site to ensure media is stored in a way that protects against accidental damage in accordance with DoDI 8500.2 or the equivalent follow-on or replacement technical guidance.
d. media, including backups, at the designated site, are stored in a way that precludes loss from natural disaster in accordance with DoDI 8500.2 or the equivalent follow-on or replacement technical guidance.
e. media containing security audit results, archives, and back up information at the designated site are stored separately from the systems that process the data in accordance with DoDI 8500.2 or the equivalent follow-on or replacement technical guidance.

f. all sensitive data being stored on removable storage media (including backup tapes) at the designated site are encrypted to provide record protection of sensitive data-at-rest in accordance with DoDI 8500.2 or the equivalent follow-on or replacement technical guidance.
g. removable information system media and information system output from the designated site be marked indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information in accordance with DoDI 8500.2 or the equivalent follow-on or replacement technical guidance.
h. digital and non-digital media maintained at the designated site be physically controlled and securely stored in accordance with DoDI 8500.2 or the equivalent follow-on or replacement technical guidance.
i. the designated site complies with DON CIO Msg DTG 091256ZOCT07, "DON Encryption of Sensitive Unclassified Data-at-Rest Guidance" or the equivalent follow-on or replacement technical guidance.

3.23 Supply Chain Security

The contractor shall conduct auditing, in accordance with the approved test plan, to verify that:

a. the designated site has a documented set of operating procedures which specifies that network devices are procured from a government approved source of supply and protects against supply chain threats.
b. the designated site complies with the documented set of procurement operating procedures for network devices in 3.23.a as provided by the government.

3.24 Excepted Networks Security

The contractor shall conduct auditing, in accordance with the approved test plan, to verify that:

a. the designated site's excepted networks, as defined in Enclosure (2) of this PWS, have implemented government provided security policies and procedures prior to connecting through a B3 boundary in accordance with DoDI 8500.2 or the equivalent follow-on or replacement technical guidance.

3.25 Physical and Environmental Protection

The contractor shall conduct auditing, in accordance with the approved test plan, to verify that:

a. the designated site develops, disseminates, and reviews/updates Physical and Environmental Protection Policies and Procedures in accordance with DoD 5200.1-R and DoDI 8500.2 or the equivalent follow-on or replacement technical guidance.
b. the designated site's documents and equipment are stored in containers or facilities with maintenance and accountability procedures in accordance with DoD

5200.1-R and DoDI 8500.2 or the equivalent follow-on or replacement technical guidance.

3.26 Contingency, Continuity of Operations, and Disaster Recovery

The contractor shall conduct auditing, in accordance with the approved test plan, to verify that:

a. the designated site has a documented set of operating procedures being implemented to maintain network performance and data protection in accordance with DoDI 8500.2 or the equivalent follow-on or replacement technical guidance.
b. the designated site has a documented disaster recovery plan in place that provides for the smooth transfer of mission critical and business essential functions to an alternate site for the duration of an event with little or no loss of operational continuity in accordance with DoDI 8500.2 or the equivalent follow-on or replacement technical guidance.

3.27 Biometrics

The contractor shall conduct auditing, in accordance with the approved test plan, to verify that:

a. the biometric systems utilized for DON at the designated site, based upon an inventory list provided by the government, are certified to be interoperable with the Federal Bureau of Investigation's (FBI) Integrated Automated Fingerprint Identification System (IAFIS).
b. that the Crossover Error Rate (CER) of all upgrades to DON biometric systems is no more than 1 in 1,000,000 in accordance with FIPS PUB 140-2 or the equivalent follow-on or replacement technical guidance.

4.0 References

See Enclosure (3) of this PWS.

5.0 Security Requirements

5.1 Visit Authorization Letter (VAL)

The contractor shall submit a request for visit authorization to the scheduled site security agency via NNWC and DON in accordance with local access request procedures.

5.2 Clearances

A Secret clearance is required for performance of services under this PWS per DD-254.

6.0 Government Furnished Information and Materials

6.1 Government Furnished Property (GFP)

The government will provide to the contractor four (4) laptop systems, which are configured to access the DON networks.

7.0 Contractor Furnished Information and Materials

The contractor shall have business office space separate from the CSIA ISOO&A Project site.

The contractor shall provide all tools, test equipment, and materials necessary to perform duties as defined in this PWS to augment the government furnished information and materials described in the PWS.

The contractor will provide all computing, administrative, printing services, and telecommunications supplies and equipment necessary to support the execution of the tasks contained in this PWS.

The contractor shall provide the designated site Information Assurance Manager (IAM) local network authorities with a description and duration of all hardware and software that will be attached to the network 10 days before the site visit.

8.0 Place of Performance

The places of performance are contained in Enclosure (1).

9.0 Travel

The contractor shall be required to travel in support of this PWS. Travel shall be handled in accordance with the Joint Federal Travel Regulations (JFTR) and the approved government plan for each designated site visit. It is estimated that the contractor shall be required to travel up to ten (10) times a year to the designated site locations listed in Enclosure (1). Travel may vary, and could exceed ten (10) trips per year based upon audit results and the contractor developed and government approved Fiscal Year Schedule identified in paragraph 2.1 of this PWS.

10.0 Acronyms and Definitions

See Enclosure (2).

Enclosure (1)

Location List for ISOO&A PWS Test/Audits

All penetration testing/auditing activities will take place at each of the locations as listed below:

a. Virginia
b. California
c. Hawaii
d. Washington
e. Florida
f. Japan

Enclosure (2)

ISOO&A PWS Acronyms and Definitions

ACRONYMS

AIS	Automated Information System
APM	Assistant Program Manager
BCP	Business Continuity Plan
BIOS	Basis Input/Output System
BPCP	Business Process Contingency Plan
BT	Boundary Transport
C2	Command and Control
CA	Certification Authority
CARS	Cyber Asset Reduction and Security
CAT	Category
CCB	Change/Configuration Control Board
CCSD	Command Communications Service Designator
CDRL	Contract Data Requirements List
CER	Crossover Error Rate
CI	Counter Intelligence
CIO	Chief Information Officer
CNA	Computer Network Attack
CND	Computer Network Defense
CNO	Chief of Naval Operations
COI	Community of Interest
COR	Contracting Officer's Representative
CONUS	Continental United States
CRL	Certificate Revocation List
CSIA	Cyber Security Information Assurance
C/S/A	Command, Services and Agencies
CTO	Communications Tasking Order
DAA	Designated Approval Authority
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
DNS	Domain Naming System
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DON	Department of the Navy
DRP	Disaster Recovery Plan
ECRR	Control Encryption for Confidentiality
DTG	Date-Time Group
FAR	Federal Acquisition Regulations
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards Publication

FY	Fiscal Year
GDA	Government Directed Action
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GIG	Global Information Grid
I&W	Indicators and Warnings
IA	Information Assurance
IAFIS	Integrated Automated Fingerprint Identification System
IAM	Information Assurance Manager
IAVA	Information Assurance Vulnerability Alert
IAVM	Information Assurance Vulnerability Management
IDS	Intrusion Detection Systems
IO	Information Operations
IP	Internet Protocol
IPS	Intrusion Prevention Systems
ISNS	Integrated Shipboard Network System
ISOO&A	Independent Security Operations and Oversight Assessment
IT	Information Technology
ITIA	Information Technology Infrastructure Architecture
ITSG	Information Technology Standards Guidance
IW	Information Warfare
JCS	Joint Chiefs of Staff
JTF	Joint Task Force
LAN	Local Area Network
MAC	Mandatory Access Control
NETWARCOM	Naval Network Warfare Command
NIPRNET	Non-classified Internet Protocol Routing Network
NIST	National Institute for Standards and Technology
NNE	Naval Networking Environment
NNWC	Naval Network Warfare Command
NOC	Network Operations Center
NSD	National Security Directive
NSTISSI	National Training Standard for Information Systems Security Infrastructure
NTISSD	National Telecommunications and Information Systems Security Directive
OCONUS	Outside of the continental United States
OpDir	Operational Directives
OPNAVINST	Chief of Naval Operations Instruction

OPSEC	Operations Security
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PMW	Program Management Warfare
POA&M	Plan of Action & Milestones (POA&M)
PPSM	Ports, Protocols, and Service Management
PWS	Performance Work Statement
SECNAVINST	Secretary of the Navy Instruction
SIO	Special Information Operations
SIPRNET	Secret Internet Protocol Routing Network
SOC	Security Operations Center
SPAWAR	Space and Naval Warfare Command
TB	Terabyte
USN	United States Navy
UTNProtect	Navy Unclassified Trusted Network Protection
VAL	Visit Authorization Letter
VV&R	Verification, Validation and Reporting
WAN	Wide Area Network

DEFINITIONS

Access. A specific type of interaction between a subject (i.e., person, process, or input device) and an object (i.e., an Automated Information Systems (AIS) resource such as a record, file, program, output device) that results in the flow of information from one to the other. Also, the ability and opportunity to obtain knowledge of classified, sensitive unclassified, or unclassified information (DoD Directive 5200.28).

Audit. The process of collecting and evaluating evidence of an organization's information systems, practices, and operations.

Automated Information Systems. Systems which create, prepare, process, or manipulate information in electronic form, and include computers, word processing systems, other electronic information handling systems, and associated equipment (National Telecommunications and Information Systems Security Policy (NTISSP) No. 200). An assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information (DoD Directive 5200.28).

Biometric System. A biometric system is essentially a pattern recognition system which recognizes a user by determining the authenticity of a specific anatomical or behavioral characteristic possessed by the user.

Black List. A list or register of persons who, for one reason or another, are being denied a particular privilege, service, mobility, access or recognition to one or more information technology systems. United States Navy Black Lists Location/Guidance: (URL: https://www.ncdoc.navy.mil/restricted/lists_released.shtml)

Blue Teaming. An independent and focused, threat –based effort by an interdisciplinary, neutral force using active and passive capabilities based on formal, time-bounded tasking to expose and exploit vulnerabilities of friendly forces. (Chairman of Joint Chief of Staff Instruction (CJCSI) 6510.01B Chg-1).

Category (CAT). A grouping of classified or sensitive unclassified information to which an additional restrictive label is applied for signifying that personnel are granted access to the information only if they have formal access approval or other applicable authorization (e.g., proprietary information, for official use only, compartmented information) (DoD Directive 5200.28).

CAT I severity category. Assigned to findings that allow primary security protections to be bypassed, allowing immediate access by unauthorized personnel or unauthorized assumption of super-user privileges. An Authority to Operate (ATO) will not be granted while CAT-I weaknesses are present.

CAT II severity category. Assigned to findings that have a potential to lead to unauthorized system access or activity. CAT-II findings that have been satisfactorily mitigated will not prevent an ATO from being granted.

CAT III severity category. Assigned to findings that may impact IA posture but are not required to be mitigated or corrected in order for an ATO to be granted.

Certification Authority (CA). An organization that determines the extent to which an IT system, component or site meets a prescribed set of technical and non-technical information assurance (IA) requirements.

Communications Security (COMSEC). Protective measures taken to deny unauthorized persons information derived from telecommunications of the US Government related to national security and to ensure the authenticity of such communications. Such protection results from the application of security measures (including crypto security, transmission security, and emissions security) to telecommunications systems generating, handling, processing, or using classified or sensitive government or government-derived information, the loss of which could adversely affect the national security interest. It also includes the application of physical security measures to COMSEC information or materials (National Telecommunications and Information Systems Security Directive (NTISSD) No. 600).

Computer. A machine capable of accepting, performing calculations on, or otherwise manipulating or storing data. It usually consists of arithmetic and logical units and a control unit, and may have input and output devices and storage devices (DoD Directive 5200.28).

Computer Network Attack (CNA). Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves (DoD Directive 3600.1).

Computer Network Defense (CND). Measures taken to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction (CJCSI 6510.01B Chg-1).

Counter Intelligence (CI). Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities (Joint Pub 1-02).

Critical Infrastructures. Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both government and private (Presidential Decision Directive-63).

Crossover Error Rate (CER). A comparison metric for different biometric devices and technologies. It is the error rate at which the false acceptance rate (FAR) equals the false rejection rate (FRR). As an identification device becomes more sensitive or accurate, its FAR decreases while its FRR increases. The CER is the point at which these two rates are equal, or cross over.

Data. Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as characters or analog quantities to which meaning is or might be assigned (Joint Pub 1-02).

Defense-in-Depth Boundary Definitions. Defense in depth is a strategy in which multiple layers of defense are placed throughout an Information Technology (IT) system. It addresses security vulnerabilities in personnel, technology and operations for the duration of the system's lifecycle.

Defense Information Infrastructure (DII). The DII is the shared or interconnected system of computers, communications, data, applications, security, people, training, and other support structure, serving the Navy's local and worldwide information needs. The DII (1) connects Navy mission support, command and control, and intelligence computers and users through voice, data, imagery, video, and multimedia services, and (2) provides information processing and value-added services to subscribers over the Defense Information Systems Network. Unique user data, information, and user applications are not considered part of the DII (CJCSI 6510.01B Chg-1).

Defensive Information Operations. The Defensive Information Operations (IO) process integrates and coordinates policies and procedures, operations, personnel, and technology to protect information and to defend information systems. Defensive IO are conducted through information assurance (IA), physical security, operations security, counter deception, counter psychological operations, counter intelligence, electronic protect, and special IO (SIO). Defensive IO objectives ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and systems for their own purposes (CJCSI 6510.01B Chg-1).

Disaster Recovery Plan (DRP). Is sometimes referred to as a business continuity plan (BCP) or business process contingency plan (BPCP). Describes how an organization is to deal with potential disasters.

Date Time Group (DTG) Indicator. Naval messages are identified by originator and date time group (DTG). For example, "USS NEVERSAIL" (typed in the From line of the message) is the originator. The DTG "1022332" (10th day at 2233 hours in Zulu time), "OCT 93" (the month and year) will be typed as "102233Z OCT 93." The "Z" represents Greenwich Mean Time and is standard throughout DOD. The DTG is assigned by the communication office at the time the message is released. Messages are filed by month in DTG sequence.

Domain Credentials. Credentials that are tied to a user to authenticate access.

Event. Any suspicious occurrence affecting an information system that has not been assessed to be an incident (CJCSI 6510.01B Chg-1).

Excepted Networks. Assets identified to remain outside of the Navy's enterprise networks (i.e. ISNS, One-Net) by Cyber Asset Reduction and Security (CARS) but have a legitimate

reason for use and support are granted this status. This means they have authorization to continue operating outside the enterprise.

Green Teaming. An independent and focused, threat–based effort by an interdisciplinary, simulated cooperative vulnerability scan using active and passive capabilities based on formal, time-bounded tasking to expose and exploit vulnerabilities of friendly forces. (CJCSI 6510.01B Chg-1).

Incident. An assessed event of attempted entry, unauthorized entry, and/or an information attack on an automated information system (AIS). It includes unauthorized probing, browsing; disruption, or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to system hardware, firmware, or software characteristics with or without the user's knowledge, instruction, or intent (e.g., malicious logic). (Also refer to security incident) (CJCSI 6510.01B Chg-1).

Indications and Warning (I&W). Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied military, political, or economic interests or to US citizen's abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear/non-nuclear attack on the United States, its overseas forces, or allied nations; hostile reactions to United States reconnaissance activities; terrorist attacks; and other similar events (CJCSI 6510.01B Chg-1).

Information.

a. Facts, data, or instructions in any medium or form (DoD Directive 3600.1).
b. Unprocessed data of every description, which may be used in the production of intelligence.
c. The meaning that a human assigns to data by means of the known conventions used in their representation (Joint Pub 1-02).

Information Assurance (IA). IO that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities (DoD Directive 3600.1).

Information Assurance Vulnerability Alert (IAVA). The comprehensive distribution process for notifying Command, Services, and Agencies (C/S/A) about vulnerability alerts and countermeasures information. The IAVA process requires C/S/A receipt acknowledgement and provides specific time parameters for implementing appropriate countermeasures depending on the criticality of the vulnerability. Defense Information Systems Agency (DISA) manages the IAVA process for Navy.

Information Operations. Actions taken to affect adversary information and information systems while defending one's own information and information system (DoD Directive 3600.1).

Information Systems.

a. The entire infrastructure, organization, personnel and components that collect, process, store, transmit, display, disseminate and act on information (DoD Directive 3600.1).
b. Any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data and includes computer software, firmware, and hardware (National Security Directive (NSD)-42).
c. The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information (CJCSI 3210.01).
d. The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual (DoD Directive 5200.28).

Information Warfare (IW). IO conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries (DoD Directive 3600.1).

Intrusion. Unauthorized access to an information system (CJCSI 6510.01B Chg-1).

Need to Know. When used by government and other organizations (particularly those related to the military or espionage), describes the restriction of data which is considered very sensitive. Under need-to-know restrictions, even if one has all the necessary official approvals (such as a security clearance) to access certain information, one would not be given access to such information, or read into a clandestine operation, unless one has a specific *need to know*; that is, access to the information must be necessary for the conduct of one's official duties.

Network. A network is composed of a communications medium and all components attached to that medium whose responsibility is the transference of information. Such components may include AIS's, packet switches, telecommunications controllers, key distribution centers, and technical control devices (DoD Directive 5200.28).

Operations Security (OPSEC). A process that identifies critical information by analyzing friendly actions attendant to military operations and other activities, and then implements procedures to prohibit disclosure of this critical information to an adversary (Joint Pub 1-02).

Red Teaming. An independent and focused, threat based effort by an interdisciplinary, simulated adversarial force using active and passive capabilities based on formal, time bounded tasking to expose and exploit vulnerabilities of friendly forces (CJCSI 6510.01B Chg-1).

Risk. A combination of the likelihood that a threat shall occur, the likelihood that a threat occurrence shall result in an adverse impact, and the severity of the resulting adverse impact (DoD Directive 5200.28).

Security Incident. An attempt to exploit a national security system such that the actual or potential adverse effects may involve fraud, waste, or abuse; compromise of information; loss or damage of property or information; or denial of service. Security incidents include penetration of computer systems, exploitation of technical and administrative vulnerabilities, and introduction of computer viruses or other forms of malicious code (NSTISSD 503). (A security incident may also involve a violation of law. If a violation of law is evident or suspected, the incident must also be reported to both security and law enforcement organizations for appropriate action.)

Security Incident Response. Actions conducted to resolve information systems security incidents and protect national security systems (NSTISSD 503).

Severity Category. The category a Certification Authority (CA) assigns to a system security weakness or shortcoming as part of a certification analysis to indicate the risk level associated with the security weakness and the urgency with which the corrective action must be completed. Severity categories are expressed as "Category (CAT) I, CAT II, or CAT III," with CAT I indicating the greatest risk and urgency. Severity categories are assigned after consideration of all possible mitigation measures that have been taken within system design/architecture limitations for the DoD IS in question.

Standardized Image. An exact software replica of a preconfigured computer, to ensure additional computers will be configured in the same manner at the time the image was taken.

State of the Shelf. The collection of all commercially available hardware/software components which provide a level of performance equal to or greater than 65% of the performance commercially available at the time such a component is deployed and refreshed. (NMCI Contract N00024-00-D-6000, Awarded 6 October 2000). This citation may be located at the following URL: http://demo.olivesoftware.com/Olive/ODE/NCMI/default.aspx?href=Contract%2F1600%2F01%2F03&pageno=1&entity=Ar00100&view=entity

Strategic Computer Network Attack (CNA). CNAs that cross-unified command, Service, or agency borders, or that attack with widespread or critical effects to the Defense Information Infrastructure (DII).

Supply Chain. A system of organizations, people, technology, activities, information and resources involved in moving a product or service from supplier to customer.

Verify. To establish the truth, accuracy, or reality of a claim.

Vulnerability. A weakness in an information system, security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system (CJCSI 6510.01B Chg-1).

Vulnerability Analysis. The systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation (NSTISSI No. 4009).

White List. A list or register of entities that, for one reason or another, are being provided a particular privilege, service, mobility, access or recognition to an information technology system. Navy White List Guidance: Date-Time Group (DTG): 241757Z APR 09 (URL: www.doncio.navy.mil/Download.aspx?AttachID=967)

Enclosure (3)

ISOO&A PWS References

a. Chairman, Joint Chiefs of Staff Instruction (CJCSI) _6510.01E, Information Assurance (IA) and Computer Network Defense (CND), 15 August 2007.
b. Code of Federal Regulations (CFR) 48, Vol. 1, Federal Acquisition Regulations System, 1 October 2008.
c. DoDD 8500.1E, "Information Assurance (IA), 23 April 2007.
d. CJCSI 6510.01E, Information Assurance and Computer Network Defense, 12 August 2008.
e. Naval Sea Systems Command (NAVSEA) Instruction 5511.32 series (Safeguarding of Naval Nuclear Propulsion Information (NNPI), July 2005 (U/NOFORN).
f. DODD 8570.1, Information Assurance Training, Certification, and Workforce Management, 23 April 2007.
g. SECNAVINST 5239.19, "Computer Network Incident Response and Reporting Requirements," March 2008.
h. SECNAVINST 5239.3B DON IA Policy, 17 June 2009.
i. OPNAVINST 5239.1C, Navy Information Assurance Program, 20 August 2008.
j. DoDI 5200.1-R, "Information Security Program," January 1997
k. DoDD 8530.1 Computer Network Defense (CND) 8 January 2001.
l. DoDI 8530.2 "Support to Computer Network Defense" (CND), 9 March 2001
m. DoDI 8500.2, "IA implementation," 6 February 2003.
n. SECNAV M-5239.1, "Information Assurance Manual," 20 August 2008.
o. DoD 8570.01-M, Information Assurance Workforce Improvement. Program," 19 December 2005.
p. SECNAV M-5510.36, "DON Information Security Program Manual," 30 June 06
q. DODI 8551.1, "Ports, Protocols, and Service Management," 13 August 2004.
r. CNSS 1253, "The Committee on National Security Systems Instruction 1253," October 2009.
s. DON CIO Information Technology Standards Guidance (ITSG), 5 April 1999.
t. DON CIO Information Technology Infrastructure Architecture (ITIA), 16 March 1999.
u. DoDI 8520.2, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," 1 April 2004.
v. NIST SP 800-53 Rev. 3, "National Institute of Standards and Technology," August 2009.
w. NIST SP 800-81, "Secure Domain Name System (DNS) Deployment Guide," May 2006.
x. NIST SP 800-115, "Technical Guide to Information Security Testing and Assessment," September 2008.
y. DON CIO Msg DTG 091256ZOCT07, "DON Encryption of Sensitive Unclassified Data-at-Rest Guidance," October 2007.
z. FIPS 140-1, "Security Requirements for Cryptographic Modules," 11 January 2004

CONTRACT DATA REQUIREMENTS LIST (CDRL)

(*1 Data Item*)

Form Approved
OMB No. 0704-0188

A. CONTRACT LINE ITEM NO.	B. EXHIBIT	C. CATEGORY:
TBD	A	**TDP** ____ **TM** ____ **OTHER** (CSIA) Cyber Sec. Info. Assurance

D. SYSTEM/ITEM	E. CONTRACT/PR NO.	F. CONTRACTOR
ISOO&A	TBD	TBD

1. DATA ITEM NO.	2. TITLE OF DATA ITEM	3. SUBTITLE	17. PRICE GROUP
IAS001	Standard Report	N/A	

4. AUTHORITY (*Data Acquisition Document No.*)	5. CONTRACT REFERENCE	6. REQUIRING OFFICE	18. ESTIMATED TOTAL PRICE
N/A	PWS Para 2.4.1.1	SPAWAR	

7. DD 250 REQ	9. DIST STATEMENT	10. FREQUENCY	12. DATE OF FIRST SUBMISSION	14. DISTRIBUTION
(5)	F	PWS Para 2.4.1.1	PWS Para 2.4.1.1	
8. APP CODE		**11. AS OF DATE**	**13. DATE IF SUBSEQUENT SUBM.**	a. ADDRESSEE
A		N/A	PWS Para 2.4.1.1	

b. COPIES		
Draft	Final	
	Reg	Repro

16. REMARKS

The Contractor shall submit Standard Reports to the Contracting Officer Representative (COR) and include the following:

- Detailed results of each penetration test/audit executed in accordance with the government approved test plan
- Any variances from the policy/standard/instruction governing the tasks in PWS, Para 3.0
- A summary of all recurring administrative issues experienced during the test/audit (e.g. site access issues, network access issues, etc.)

Block 9: Directed by Contracting Officer (CO) or Contracting Officer Representative (COR)

Block 14: Electronically Delivered-Reproducible format

a. ADDRESSEE	Draft	Final Reg	Final Repro
BLK 16			
15. TOTAL ——▶			

G. PREPARED BY	H. DATE	I. APPROVED BY	J. DATE
	01/23/2010		

CONTRACT DATA REQUIREMENTS LIST (CDRL) (*1 Data Item*)	*Form Approved OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Services Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **Please do not return your form to the above organization. Send completed form to the Government Issuing Contracting Officer for the Contract/PR No. listed in Block E.**

A. CONTRACT LINE ITEM NO.	B. EXHIBIT	C. CATEGORY:		
TBD	A	**TDP** ____	**TM** _____	**OTHER** (CSIA) Cyber Sec. Info. Assurance

D. SYSTEM/ITEM	E. CONTRACT/PR NO.	F. CONTRACT
ISOO&A	TBD	TBD

1. DATA ITEM NO.	2. TITLE OF DATA ITEM	3. SUBTITLE	17. PRICE GROUP
IAS002	Exception Report	N/A	

4. AUTHORITY (*Data Acquisition Document No.*)	5. CONTRACT REFERENCE	6. REQUIRING OFFICE	18. ESTIMATED TOTAL PRICE
N/A	PWS Para 2.4.1.2	SPAWAR	

7. DD 250 REQ	9. DIST STATEMENT	10. FREQUENCY	12. DATE OF FIRST SUBMISSION
(5)	F	PWS Para 2.4.1.1.	PWS Para 2.4.1.2

8. APP CODE	11. AS OF DATE	13. DATE IF SUBSEQUENT SUBM.
A	N/A	PWS Para 2.4.1.2

16. REMARKS

The Contractor shall submit Exception Reports to the Contracting Officer Representative (COR) and include the following:

- The identity of the penetration test/audit that resulted in the discovery of the exception (CAT-1 class finding) that posed the risk to the enterprise security posture.
- Detailed results of each CAT-1 class finding in accordance with the government approved test plan.

Block 9: Directed by Contracting Officer (CO) or Contracting Officer Representative (COR)

Block 14: Electronically Delivered-Reproducible format

14. DISTRIBUTION	b. COPIES		
a. ADDRESSEE	Draft	Final	
		Reg	Repro
BLK 16			
15. TOTAL ⟶			

G. PREPARED BY	H. DATE	I. APPROVED BY	J. DATE
	01/23/2010		

CONTRACT DATA REQUIREMENTS LIST (CDRL) (*1 Data Item*)	*Form Approved OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Services Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **Please do not return your form to the above organization. Send completed form to the Government Issuing Contracting Officer for the Contract/PR No. listed in Block E.**

A. CONTRACT LINE ITEM NO.	B. EXHIBIT	C. CATEGORY:			
TBD	A	**TDP** ____	**TM** _____	**OTHER** (CSIA) Cyber Sec. Info. Assurance	
D. SYSTEM/ITEM	**E. CONTRACT/PR NO.**	**F. CONTRACT**			
ISOOA	TBD	TBD			
1. DATA ITEM NO.	**2. TITLE OF DATA ITEM**	**3. SUBTITLE**		**17. PRICE GROUP**	
IAS003	Monthly Summary Report	N/A			
4. AUTHORITY (*Data Acquisition Document No.***)**	**5. CONTRACT REFERENCE**	**6. REQUIRING OFFICE**		**18. ESTIMATED TOTAL PRICE**	
N/A	PWS Para 2.4.2.1	SPAWAR			

7. DD 250 REQ	9. DIST STATEMENT	10. FREQUENCY	12. DATE OF FIRST SUBMISSION
(5)	F	PWS Para 2.4.2.1	PWS Para 2.4.2.1
8. APP CODE		**11. AS OF DATE**	**13. DATE IF SUBSEQUENT SUBM.**
A		N/A	PWS Para 2.4.2.1

14. DISTRIBUTION			
a. ADDRESSEE	b. COPIES		
	Draft	Final	
		Reg	Repro
BLK 16			

16. REMARKS

The Contractor shall submit Monthly Summary Report to the Contracting Officer Representative (COR) and include the following:

- A summary of all activities accomplished during the month
- A summary of all recurring administrative issues experienced during the month (e.g. site access issues, network access issues, etc.)
- A summary of labor and travel categorized by:
  - Monthly initial projected Labor Hours/Costs, ODC, Travel
  - Monthly actual Labor Hours/Costs, ODC, Travel (Burn Rate)
  - Explanation of variances between initial monthly projected and actual Labor Hours/Costs, ODC, and Travel
  - Future monthly projected expenditures (Labor Hours/Costs, ODC, Travel)

Block 9: Directed by Contracting Officer (CO) or Contracting Officer Representative (COR)

Block 14: Electronically Delivered-Reproducible format

15. TOTAL ——►

G. PREPARED BY	H. DATE	I. APPROVED BY	J. DATE
	01/23/2010		

CONTRACT DATA REQUIREMENTS LIST (CDRL) (*1 Data Item*)	*Form Approved OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Services Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **Please do not return your form to the above organization. Send completed form to the Government Issuing Contracting Officer for the Contract/PR No. listed in Block E.**

A. CONTRACT LINE ITEM NO.	B. EXHIBIT	C. CATEGORY:		
TBD	A	**TDP** ____	**TM** _____	**OTHER** (CSIA) Cyber Sec. Info. Assurance

D. SYSTEM/ITEM	E. CONTRACT/PR NO.	F. CONTRACTOR
ISOO&A	TBD	TBD

1. DATA ITEM NO.	2. TITLE OF DATA ITEM	3. SUBTITLE	17. PRICE GROUP
IAS004	Annual Project Report	N/A	

4. AUTHORITY (*Data Acquisition Document No.*)	5. CONTRACT REFERENCE	6. REQUIRING OFFICE	18. ESTIMATED TOTAL PRICE
N/A	PWS Para 2.4.2.2	SPAWAR	

7. DD 250 REQ	9. DIST STATEMENT	10. FREQUENCY	12. DATE OF FIRST SUBMISSION	14. DISTRIBUTION
(5)	F	PWS Para 2.4.2.2	PWS Para 2.4.2.2	
8. APP CODE		**11. AS OF DATE**	**13. DATE IF SUBSEQUENT SUBM.**	a. ADDRESSEE
A		N/A	PWS Para 2.4.2.2	

b. COPIES		
Draft	Final	
	Reg	Repro

16. REMARKS

The Contractor shall submit Annual Project Summary to the Contracting Officer Representative (COR) and include the following:

- A summary of all exception reports submitted during the annual contract year, including suggestions (e.g. best practices, industry standards, lessons learned, and other relevant observations) for improving the failures contributing to the exception.
- A summary of all recurring administrative issues experienced during the annual contract year (e.g. site access issues, network access issues, etc.)
- A summary of labor and travel categorized by:
  - Annual initial projected Labor Hours/Costs, ODC, Travel
  - Annual actual Labor Hours/Costs, ODC, Travel (Burn Rate)
  - Explanation of variances between initial annual projected and actual Labor Hours/Costs, ODC, Travel
  - Future annual projected Labor Hours/Costs, ODC, Travel

Block 9: Directed by Contracting Officer (CO) or Contracting Officer Representative (COR)

Block 14: Electronically Delivered-Reproducible format

a. ADDRESSEE	Draft	Final Reg	Final Repro
BLK 16			
15. TOTAL ——►			

G. PREPARED BY	H. DATE	I. APPROVED BY	J. DATE
	01/23/2010		